

# Distance Constraint Satisfaction Problems

Manuel Bodirsky\*   Victor Dalmau†   Barnaby Martin‡   Michael Pinsker§

May 25, 2011

## Abstract

We study the complexity of constraint satisfaction problems for templates  $\Gamma$  that are first-order definable in  $(\mathbb{Z}; \text{succ})$ , the integers with the successor relation. In the case that  $\Gamma$  is locally finite (i.e., the Gaifman graph of  $\Gamma$  has finite degree), we show that  $\Gamma$  is homomorphically equivalent to a structure with a certain majority polymorphism (which we call *modular median*) and the CSP for  $\Gamma$  can be solved in polynomial time, or  $\Gamma$  is homomorphically equivalent to a finite transitive structure, or the CSP for  $\Gamma$  is NP-complete. Assuming a widely believed conjecture from finite domain constraint satisfaction (we require the *tractability conjecture* by Bulatov, Jeavons and Krokhin in the special case of *transitive* finite templates), this proves that those CSPs have a complexity dichotomy, that is, are either in P or NP-complete.

## 1 Introduction

Constraint satisfaction problems appear naturally in many areas of theoretical computer science, for example in artificial intelligence, optimization, computer algebra, computational biology, computational linguistics, and type systems for programming languages. Such problems are typically NP-hard, but sometimes they are polynomial-time tractable. The question as to which CSPs are in P and which are hard has stimulated a lot of research in the past 10 years. For pointers to the literature, there is a recent collection of survey articles [10].

The *constraint satisfaction problem CSP* for a fixed (not necessarily finite) structure  $\Gamma$  with a finite relational signature  $\tau$  is the computational problem to decide whether a given primitive positive sentence is true in  $\Gamma$ . A formula is *primitive positive* if it is of the form  $\exists x_1, \dots, x_n. \psi_1 \wedge \dots \wedge \psi_m$  where  $\psi_i$  is an atomic formula over  $\Gamma$ , i.e., a formula of the form  $R(y_1, \dots, y_j)$  for a relation symbol  $R$  of a relation from  $\Gamma$ . The structure  $\Gamma$  is also called the *template* of the CSP.

The class of problems that can be formulated as a CSP for a fixed structure  $\Gamma$  is very large. It can be shown that for every computational problem there is a structure  $\Gamma$  such that the CSP for  $\Gamma$  is equivalent to this problem under polynomial-time Turing reductions [3]. This makes it very

---

\*CNRS / LIX UMR 7161, École Polytechnique, Greater Paris, France. Manuel Bodirsky research has received support from the European Research Council under the European Community's Seventh Framework Programme (FP7/2007-2013 Grant Agreement no. 257039).

†Universitat Pompeu Fabra, Barcelona, Spain. Victor Dalmau research has been supported by the MCINN grant TIN2010-20967-C04-02.

‡School of Engineering and Computing Sciences, Durham University, Durham, UK. Barnaby Martin supported by EPSRC grant EP/G020604/1.

§Équipe de Logique Mathématique, Université Denis-Diderot Paris 7, France. Michael Pinsker is grateful for support through Erwin-Schrödinger-Fellowship J2742-N18 and project P21209 of the Austrian Science Fund (FWF), as well as through an APART-fellowship of the Austrian Academy of Sciences.

unlikely that we can give good descriptions of all those  $\Gamma$  where the CSP for  $\Gamma$  is in P. In contrast, the class of CSPs for a *finite* structure  $\Gamma$  is quite restricted, and indeed it has been conjectured that the CSP for  $\Gamma$  is either in P or NP-complete in this case [12]. So it appears to be natural to study the CSP for classes of infinite structures  $\Gamma$  that share good properties with finite structures.

In graph theory and combinatorics, there are two major concepts of *finiteness* for infinite structures. The first is  $\omega$ -categoricity: a countable structure is  $\omega$ -categorical if and only if its automorphism group has for all  $n$  only finitely many orbits in its natural action on  $n$ -tuples [9, 19, 16]. This property has been exploited to transfer techniques that were known to analyze the computational complexity of CSPs with finite domains to infinite domains [6, 5, 7]; see also the introduction of [2].

The second concept of finiteness is the property of an infinite graph or structure to be *locally finite* (see Section 8 in [11]). A graph is called locally finite if every vertex is contained in a finite number of edges; a relational structure is called locally finite if its Gaifman graph (definition given in Section 2) is locally finite. Many conjectures that are open for general infinite graphs become true for locally finite graphs, and many results that are difficult become easy for locally finite graphs.

In this paper, we initiate the study of CSPs with locally finite templates by studying locally finite templates that have a first-order definition in  $(\mathbb{Z}; \text{succ})$ , where  $\text{succ} = \{(x, y) \mid x = y + 1\}$  is the successor relation on the integers.

As an example, consider the directed graph with vertex set  $\mathbb{Z}$  which has an edge between  $x$  and  $y$  if the difference,  $y - x$ , between  $x$  and  $y$  is either 1 or 2. This graph can be viewed as the structure  $(\mathbb{Z}; \text{Diff}_{\{1,3\}})$  where  $\text{Diff}_{\{1,3\}} = \{(x, y) \mid x - y \in \{1, 3\}\}$ , which has a first-order definition over  $(\mathbb{Z}; \text{succ})$  since  $R_{\{1,2\}}(x, y)$  iff

$$\text{succ}(x, y) \vee \exists u, v. \text{succ}(x, u) \wedge \text{succ}(u, v) \wedge \text{succ}(v, y) .$$

Another example is the undirected graph  $(\mathbb{Z}; \text{Dist}_{\{1,2\}})$  with vertex set  $\mathbb{Z}$  where two integers  $x, y$  are linked if the *distance*,  $|y - x|$ , is one or two.

Structures with a first-order definition in  $(\mathbb{Z}; \text{succ})$  are particularly well-behaved from a model-theoretic perspective: all of those structures are strongly minimal [19, 16], and therefore uncountably categorical. Uncountable models of their first-order theory will be saturated; for implications of those properties for the study of the CSP, see [4]. In some sense,  $(\mathbb{Z}; \text{succ})$  constitutes one of the simplest infinite structures that is not  $\omega$ -categorical.

The corresponding class of CSPs contains many natural combinatorial problems. For instance, the CSP for the structure  $(\mathbb{Z}; R_{\{1,3\}})$  is the computational problem consisting to label the vertices of a given directed graph  $G$  such that if  $(x, y)$  is an arc in  $G$ , then the difference between the label for  $x$  and the label for  $y$  is one or three. It will follow from our general results that this problem is in P. The CSP for the undirected graph  $(\mathbb{Z}; \text{Dist}_{\{1,2\}})$  is exactly the 3-coloring problem, and hence, NP-complete. This is readily seen if one observes that any homomorphism of a graph  $G$  into the template modulo 3 gives rise to a 3-coloring of  $G$ . In general, the problems that we study in this paper have the flavor of assignment problems where we have to assign integers to variables such that various given constraints on differences and distances (and Boolean combinations thereof) between variables are satisfied. We therefore call the class of CSPs whose template is locally finite and definable over  $(\mathbb{Z}; \text{succ})$  *distance CSPs*.

In Section 6 we prove the following classification result for distance CSPs.

**Theorem 1** *Let  $\Gamma$  be a locally finite structure with a first-order definition in  $(\mathbb{Z}; \text{succ})$  that is not homomorphically equivalent to a finite structure. Then either*

- *The CSP for  $\Gamma$  is NP-complete.*

- $\Gamma$  has a modular median polymorphism (see Section 5), and the CSP for  $\Gamma$  is in P.

If a locally finite structure  $\Gamma$  with a first-order definition in  $(\mathbb{Z}; \text{succ})$  has a finite core, then a widely accepted conjecture about finite domain CSPs implies that the CSP for  $\Gamma$  is either NP-complete or in P. In fact, for this we only need the special case of the conjecture of Feder and Vardi [12] that states that the CSP for finite templates with a transitive automorphism group is either in P or NP-complete (see Section 7 for details).

Our theorem shows that if  $\Gamma$  is not homomorphically equivalent to a finite core, then the CSP for  $\Gamma$  is NP-complete, or that  $\Gamma$  has a certain majority polymorphism, which we call *modular median* (defined in Section 5), and the CSP for  $\Gamma$  can be solved in polynomial time by local consistency techniques. Polynomial-time tractability results based on local consistency were previously only known for finite or  $\omega$ -categorical templates; we use the assumption that templates for distance CSPs are locally finite to extend the technique to non- $\omega$ -categorical templates.

On the way to our classification result we derive several facts about structures definable in  $(\mathbb{Z}; \text{succ})$ , and automorphisms and endomorphisms of these structures, which might be of independent interest in model theory, universal algebra, and combinatorics. For example, we show that every injective endomorphism of a connected locally finite structure  $\Gamma$  with a first-order definition in  $(\mathbb{Z}; \text{succ})$  is either of the form  $x \mapsto -x + c$  or of the form  $x \mapsto x + c$  for some  $c \in \mathbb{Z}$ .

## 2 Preliminaries

A finite relational signature  $\tau$  is a finite set of relation symbols  $R_i$ , each of which has an associated arity  $k_i$ . A (relational) structure  $\Gamma$  consists of a set  $D$  (the domain) together with a relation  $R_i^\Gamma \subseteq D^{k_i}$  for each relation symbol  $R_i$  from  $\tau$ . We consider only finite signature structures in this paper.

For  $x, y \in \mathbb{Z}$ , let  $d(x, y)$  be the distance between  $x$  and  $y$ , that is,  $|x - y|$ . The relation  $\{(x, y) \mid y = x + 1\}$  is denoted by  $\text{succ}$ , and the relation  $\{(x, y) \mid d(x, y) = 1\}$  is denoted by  $\text{sym-succ}$ . A  $k$ -ary relation  $R$  is said to be *first-order (fo) definable* in the  $\tau$ -structure  $\Gamma$  if there is an fo- $\tau$ -formula  $\phi(x_1, \dots, x_k)$  such that  $R = \{(x_1, \dots, x_k) : \Gamma \models \phi(x_1, \dots, x_k)\}$ . A structure  $\Delta$  is said to be fo-definable in  $\Gamma$  if each of its relations is fo-definable in  $\Gamma$ . For example,  $(\mathbb{Z}; \text{sym-succ})$  is fo-definable in  $(\mathbb{Z}; \text{succ})$  (though the converse is false).

The structure induced by a subset  $S$  of the domain of  $\Gamma$  is denoted by  $\Gamma[S]$ . We say that a structure is *connected* if it cannot be written as the disjoint union of two other structures. The *Gaifman graph* of a relational structure  $\Gamma$  with domain  $D$  is the following undirected graph: the vertex set is  $D$ , and there is an edge between distinct elements  $x, y \in D$  when there is a tuple in one of the relations of  $\Gamma$  that has both  $x$  and  $y$  as entries. A structure  $\Gamma$  is readily seen to be connected if and only if its Gaifman graph is connected. The *degree* of a structure  $\Gamma$  is defined to be the degree of the Gaifman graph of  $\Gamma$ . The degree of a relation  $R \subseteq \mathbb{Z}^k$  is defined to be the degree of the structure  $(\mathbb{Z}; R)$ . Throughout the paper,  $\Gamma$  will be a finite-degree relational structure with an fo definition in  $(\mathbb{Z}; \text{succ})$ . The notation  $(\Gamma, R)$  indicates the expansion of  $\Gamma$  with the new relation  $R$ .

An fo-formula  $\Theta$  is *primitive positive* (pp) if it is of the form  $\exists x_1, \dots, x_i. \theta(x_1, \dots, x_i, x_{i+1}, \dots, x_j)$  where  $\theta$  is a conjunction of atoms. Note that we consider the boolean false  $\perp$  to be a pp-formula, and we always allow equalities in pp-formulas. A pp-sentence is a pp-formula with no free variables. Suppose  $\Gamma$  is a finite structure over a finite signature with domain  $D := \{a_1, \dots, a_s\}$ . Let  $\theta_\Gamma(x_1, \dots, x_s)$  be the conjunction of the positive facts of  $\Gamma$ , where the variables  $x_1, \dots, x_s$  correspond to the elements  $a_1, \dots, a_s$ . That is,  $R(x_{\lambda_1}, \dots, x_{\lambda_k})$  appears as an atom in  $\theta_\Gamma$  iff  $(a_{\lambda_1}, \dots, a_{\lambda_k}) \in R^\Gamma$ .

Define the pp-sentence  $\exists x_1 \dots x_s. \theta_\Gamma(x_1, \dots, x_s)$  to be the *canonical query* of  $\Gamma$ . Conversely, for a pp-sentence  $\Theta := \exists x_1 \dots x_s. \theta(x_1, \dots, x_s)$  we build the *canonical database*  $\Gamma_\Theta$  to be the structure with domain  $\{x_1, \dots, x_s\}$  of which  $\theta(x_1, \dots, x_s)$  lists the positive facts.

For a structure  $\Gamma$  over a finite signature,  $\text{CSP}(\Gamma)$  is the computational problem to decide whether a given pp-sentence is true in  $\Gamma$ . It is not hard to see that  $\text{CSP}(\Delta) \leq_P \text{CSP}(\Gamma)$  for any  $\Gamma$  and  $\Delta$  with the same domain such that each of the relations of  $\Delta$  is pp-definable in  $\Gamma$  (see [18]); here,  $\leq_P$  indicates polynomial-time many-to-one reduction (in fact, logspace reductions may be used, though this is harder to see and requires the celebrated result of [20]).

Let  $\Gamma$  and  $\Delta$  be  $\tau$ -structures. A *homomorphism* from  $\Gamma$  to  $\Delta$  is a function  $f$  from the domain of  $\Gamma$  to the domain of  $\Delta$  such that, for each  $k$ -ary relation symbol  $R$  in  $\tau$  and each  $k$ -tuple  $(a_1, \dots, a_k)$  from  $\Gamma$ , if  $(a_1, \dots, a_k) \in R^\Gamma$ , then  $(f(a_1), \dots, f(a_k)) \in R^\Delta$ . In this case we say that the map  $f$  *preserves* the relation  $R$ . Injective homomorphisms that also preserve the complement of each relation are called *embeddings*. Surjective embeddings are called isomorphisms; homomorphisms and isomorphisms from  $\Gamma$  to itself are called *endomorphisms* and *automorphisms*, respectively. The set of automorphisms of a structure  $\Gamma$  forms a group under composition. A  $(k$ -ary) *polymorphism* of a structure  $\Gamma$  over domain  $D$  is a function  $f : D^k \rightarrow D$  such that, for all  $m$ -ary relations  $R$  of  $\Gamma$ , if  $(a_1^i, \dots, a_m^i) \in R^\Gamma$ , for all  $i \leq k$ , then  $(f(a_1^1, \dots, a_m^1), \dots, f(a_1^k, \dots, a_m^k)) \in R^\Gamma$ .

A unary function  $g$  (over domain  $D$ ) is in the *local closure* of a set of unary functions  $F$  (over domain  $D$ ) if, for every finite  $D' \subseteq D$  there is a function  $f' \in F$  such that  $g$  and  $f'$  agree on all elements in  $D'$ . We say the  $F$  *generates*  $f$  if  $f$  is in the local closure of the set  $F'$  of all functions that can be obtained from the members of  $F$  by repeated applications of composition.

If there exist homomorphisms  $f : \Gamma \rightarrow \Delta$  and  $g : \Delta \rightarrow \Gamma$  then  $\Gamma$  and  $\Delta$  are said to be *homomorphically equivalent*. It is a basic observation that  $\text{CSP}(\Gamma) = \text{CSP}(\Delta)$  if  $\Gamma$  and  $\Delta$  are homomorphically equivalent. A structure is a *core* if all of its endomorphisms are embeddings [1] – a *core*  $\Delta$  of a structure  $\Gamma$  is an induced substructure that is itself a core and is homomorphically equivalent to  $\Gamma$ . It is well-known that, if a structure has a finite core, then that core is unique up to isomorphism (the same is not true for infinite cores).

We could have equivalently defined the class of distance CSPs as the class of CSPs whose template is locally finite and first-order definable in  $(\mathbb{Z}; s)$ , where  $s$  is the unary successor *function*, since  $(\mathbb{Z}; \text{succ})$  and  $(\mathbb{Z}; s)$  fo-define the same structures. The structure  $(\mathbb{Z}; s)$  admits *quantifier elimination*; that is, for every fo-formula  $\phi(\bar{x})$  there is a quantifier-free (qf)  $\phi'(\bar{x})$  such that  $(\mathbb{Z}; s) \models \forall \bar{x}. \phi(\bar{x}) \leftrightarrow \phi'(\bar{x})$  (this is easy to prove, and can be found explicitly in [13]). Thus we may have terms in  $\phi'$  of the form  $y = s^j(x)$ , where  $s^j$  is the successor function composed on itself  $j$  times. Let  $\Gamma$  be a finite signature structure, fo-definable in  $(\mathbb{Z}; \text{succ})$ , i.e. qf-definable in its functional variant  $(\mathbb{Z}; s)$ . Let  $m$  be the largest number such that  $y = s^m(x)$  appears as a term in the qf definition of a relation of  $\Gamma$ . Consider now  $\text{CSP}(\Gamma)$ , the problem to evaluate  $\Phi := \exists x_1, \dots, x_k. \phi(x_1, \dots, x_k)$ , where  $\phi$  is a conjunction of atoms, on  $\Gamma$ . Let  $S := \{1, \dots, k \cdot (m+1)\}$ . It is not hard to see that  $\Gamma \models \Phi$  iff  $\Gamma[S] \models \Phi$ . It follows that  $\text{CSP}(\Gamma)$  will always be in NP.

### 3 Endomorphisms

The main result of this section is the following theorem.

**Theorem 2** *Let  $\Gamma$  be a relational structure with a first-order definition in  $(\mathbb{Z}; \text{succ})$  which has finite degree and which is connected. Then:*

- *The automorphism group of  $\Gamma$  equals either the automorphism group of  $(\mathbb{Z}; \text{succ})$ , or that of  $(\mathbb{Z}; \text{sym-succ})$ .*

- *Either  $\Gamma$  has a finite range endomorphism, or it has an endomorphism which maps  $\Gamma$  onto a subset of  $\mathbb{Z}$  isomorphic to a structure fo-definable in  $(\mathbb{Z}; \text{succ})$  all of whose endomorphisms are automorphisms.*

The proof of this theorem can be found at the end of this section, and makes use of a series of lemmata. We assume henceforth that  $\Gamma$  is a relational structure with a first-order definition in  $(\mathbb{Z}; \text{succ})$  which has finite degree and which is connected.

Before beginning the proof, we remark that although it is tempting to believe that the automorphism group of  $\Gamma$  equals that of  $(\mathbb{Z}; \text{sym-succ})$  iff  $\Gamma$  is fo-definable in the latter structure, this is not true: Let

$$R := \{(x, y, u, v) \in \mathbb{Z}^4 : (y = \text{succ}(x) \wedge v = \text{succ}(u)) \vee (u = \text{succ}(v) \wedge x = \text{succ}(y))\},$$

and set  $\Gamma := (\mathbb{Z}; R)$ . Clearly,  $\Gamma$  satisfies the hypotheses of Theorem 2. The function which sends every  $x \in \mathbb{Z}$  to  $-x$  is an automorphism of  $\Gamma$ , so the automorphism group of  $\Gamma$  equals that of  $(\mathbb{Z}; \text{sym-succ})$ , by Theorem 2. However,  $R$  is not fo-definable in  $(\mathbb{Z}; \text{sym-succ})$ . To see this, suppose it were definable. For every positive natural number  $i$ , let  $\text{sym-succ}^i$  be the binary relation that says that the distance between two points equals  $i$ . Then  $R$  is also definable in  $(\mathbb{Z}; \text{sym-succ}^1, \text{sym-succ}^2, \dots)$ , and even with a quantifier-free formula  $\phi$  since this structure has quantifier-elimination. Let  $n$  be the maximal natural number such that  $\text{sym-succ}^n$  occurs in  $\phi$ . Then a short moment of reflection suffices to see that  $\phi(0, 1, n+2, n+3)$  holds iff  $\phi(0, 1, n+3, n+2)$  holds, a contradiction since the former tuple is an element of  $R$  whereas the latter is not.

Denote by  $E$  the edge-relation of the Gaifman graph of  $\Gamma$ . It is clear that every endomorphism of  $\Gamma$  preserves  $E$ . We claim that there are  $0 < d_1 < \dots < d_n$  such that  $E(x, y)$  holds iff  $d(x, y) \in \{d_1, \dots, d_n\}$ . To see this, observe that if  $x, y \in \mathbb{Z}$  are connected by  $E$  and  $u, v \in \mathbb{Z}$  are so that  $d(x, y) = d(u, v)$ , then also  $u, v$  are connected by  $E$ : This is because there is an automorphism of  $(\mathbb{Z}; \text{succ})$  (and hence of  $\Gamma$ ) which sends  $\{x, y\}$  to  $\{u, v\}$  and this automorphism also preserves  $E$ . Hence, the relation  $E$  is determined by distances. Moreover, there are only finitely many distances since  $\Gamma$  is assumed to have finite degree.

**Definition 3** *We will refer to the distances defining the Gaifman graph of  $\Gamma$  as  $d_1, \dots, d_n$ . We also write  $D$  for the largest distance  $d_n$ .*

The following claim, very easy to prove, will be used a number of times.

**Claim 4**  *$\Gamma$  is connected if and only if the greatest common divisor of  $d_1, \dots, d_n$  is 1.*

PROOF: If  $d$  is the greatest common divisor of  $d_1, \dots, d_n$  it is clear that all the nodes accessible from a node  $x \in \mathbb{Z}$  are of the form  $x + c \cdot d$  where  $c \in \mathbb{Z}$ . Conversely, every node of the form  $x + c \cdot d$  is accesible from  $x$  because  $c \cdot d = c_1 \cdot d_1 + \dots + c_n \cdot d_n$  for some  $c_1, \dots, c_n \in \mathbb{Z}$ . ■

In order to lighten the notation we might use  $ex$  to denote  $e(x)$ , where  $e$  is an endomorphism of  $\Gamma$  and  $x \in \mathbb{Z}$ .

**Lemma 5** *Suppose that  $\Gamma$  is connected and of finite degree. Then there exists a constant  $c = c(\Gamma)$  such that for all endomorphisms  $e$  of  $\Gamma$  we have  $d(e(x), e(y)) \leq d(x, y) + c$  for all  $x, y \in \mathbb{Z}$ .*

PROOF: We first claim that for every  $0 < q < D$ , there exists a number  $c_q$  such that  $d(e(x), e(y)) \leq c_q$  for all endomorphisms  $e$  of  $\Gamma$  and all  $x, y \in \mathbb{Z}$  with  $d(x, y) = q$ . To see this, pick  $u, v$  with  $d(u, v) = q$  and a path between  $u$  and  $v$  in the Gaifman graph of  $\Gamma$ ; say this path has length  $l_q$ . Then, since this path is mapped to a path under any endomorphism, we have

$d(e(u), e(v)) \leq D \cdot l_q$  for all endomorphisms  $e$ . Since an isomorphic path exists for all  $x, y$  with the same distance, our claim follows by setting  $c_q := D \cdot l_q$ . Set  $c$  to be the maximum of the  $c_q$ , and let an endomorphism  $e$  and  $x, y \in \mathbb{Z}$  be given. Assume wlog that  $x < y$ . There exists  $m \geq 0$  and  $0 \leq q < D$  such that  $y = x + D \cdot m + q$ . Set  $x_r := x + D \cdot r$ , for all  $0 \leq r \leq m$ . Now

$$\begin{aligned} d(ex, ey) &\leq \sum_{0 \leq r < m} d(ex_r, ex_{r+1}) + d(ex_m, ey) \leq D \cdot m + d(ex_m, ey) \\ &\leq d(x, y) + d(ex_m, ey) \leq d(x, y) + c. \end{aligned}$$

■

Observe that a constant  $c(\Gamma)$  not only exists, but can actually be calculated given the distances  $d_1, \dots, d_n$ . In the following, we will keep the symbol  $c$  reserved for the minimal constant guaranteed by the preceding lemma.

**Lemma 6** *Let  $e$  be an endomorphism of  $\Gamma$ . If for all  $k > c + 1$  there exist  $x, y$  with  $d(x, y) = k$  and  $d(e(x), e(y)) < k$ , then  $e$  generates a finite range operation whose range has size at most  $2(c + 1)$ .*

PROOF: Let  $A \subseteq \mathbb{Z}$  be finite. We claim that  $e$  generates a function  $f_A$  which maps  $A$  into a set of diameter at most  $2c + 1$ . The lemma then follows by the following standard local closure argument: Let  $S$  be the set of all those functions  $\alpha$  whose domain is a finite interval  $[-n; n] \subseteq \mathbb{Z}$  and whose range is contained in the interval  $[-c; c]$ , and which have the property that there exists a function generated by  $e$  which agrees with  $\alpha$  on  $[-n; n]$ . By our claim,  $S$  is infinite. For functions  $\alpha, \beta$  in  $S$ , write  $\alpha \leq \beta$  iff  $\beta$  is an extension of  $\alpha$ . Clearly, the set  $S$ , equipped with this order, forms a finitely branching tree; since the tree is infinite, it has an infinite branch (this easily verified fact is called König's lemma)  $B \subseteq S$ . The branch  $B$  defines a function  $f$  from  $\mathbb{Z}$  into the interval  $[-c; c]$ ; since  $e$  generates functions which agree with  $f$  on arbitrarily large intervals of the form  $[-n; n]$ , we have that  $f$  is generated by  $e$ , too. This completes the proof.

Enumerate the pairs  $(x, y) \in A^2$  with  $x < y$  by  $(x_1, y_1), \dots, (x_r, y_r)$ . Now the hypothesis implies that there exists  $t_1$  generated by  $e$  such that  $d(t_1 x_1, t_1 y_1) \leq c + 1$ . Similarly, there exists  $t_2$  generated by  $e$  such that  $d(t_2 t_1 x_2, t_2 t_1 y_2) \leq c + 1$ . Continuing like this we arrive at a function  $t_r$  generated by  $e$  such that  $d(t_r t_{r-1} \dots t_1 x_r, t_r t_{r-1} \dots t_1 y_r) \leq c + 1$ . Now consider  $t := t_r \circ \dots \circ t_1$ . Set  $f_j := t_r \circ \dots \circ t_{j+1}$  and  $g_j := t_j \circ \dots \circ t_1$ , for all  $1 \leq j \leq r$ ; so  $t = f_j \circ g_j$ . Then, since by construction  $d(g_j(x_j), g_j(y_j)) \leq c + 1$ , we have that  $d(tx_j, ty_j) = d(f_j(g_j(x_j)), f_j(g_j(y_j))) \leq d(g_j(x_j), g_j(y_j)) + c \leq 2c + 1$  for all  $1 \leq j \leq r$ , and our claim follows. ■

**Lemma 7** *If the hypothesis of the preceding lemma does not hold, i.e., if there exists  $k > c + 1$  such that  $d(ex, ey) \geq k$  for all  $x, y$  with  $d(x, y) = k$ , then either  $e(s + D) = e(s) + D$  for all  $s \in \mathbb{Z}$  or  $e(s + D) = e(s) - D$  for all  $s \in \mathbb{Z}$ . In particular,  $e$  does not generate a finite range operation.*

PROOF: Let  $k > c + 1$  be so that  $d(ex, ey) \geq k$  for all  $x, y$  with  $d(x, y) = k$ . Let  $w \in \mathbb{Z}$  be arbitrary. Then, since  $d(e(w + k), e(w)) \geq k$ , we have  $e(w) \neq e(w + k)$ ; say wlog  $e(w + k) > e(w)$ . Since  $d(w, w + k) = k$  we have  $e(w + k) \geq e(w) + k$ . We claim that for all  $v \in \mathbb{Z}$ ,  $e(v + k) \geq e(v) + k$ . Suppose not, and say wlog that there exists  $v > w$  contradicting our claim. Then, since  $d(e(v + k), e(v)) \geq k$ , we have  $e(v + k) \leq e(v) - k$ . Take the minimal  $v$  with  $v > w$  satisfying this property. Then, by minimality, we have  $e(v - 1 + k) \geq e(v - 1) + k$ . Since by Lemma 5 we have  $d(e(v - 1 + k), e(v + k)) \leq c + 1$ , we get that  $e(v - 1) + k - c - 1 \leq e(v + k)$ . On the other hand,  $e(v) - c - 1 \leq e(v - 1)$ . Inserting this into the previous inequality, we obtain  $e(v) - c - 1 + k - c - 1 \leq e(v + k)$ , which yields  $e(v) - 2c - 2 + k \leq e(v + k)$ . By our assumption on  $v$ , we obtain  $e(v) - 2c - 2 + k \leq e(v) - k$ , which yields  $k \leq c + 1$ , a contradiction.

Set  $b := k \cdot D$ . We next claim that  $e(v + b) = e(v) + b$  for all  $v \in \mathbb{Z}$ . Since  $b$  is a multiple of  $D$  and points with distance  $D$  cannot be mapped to points with larger distance, we get that  $e(v + b) \leq e(v) + b$ . On the other hand, since  $b$  is also a multiple of  $k$  and since  $e(v + k) \geq e(v) + k$  for all  $v \in \mathbb{Z}$ , we obtain  $e(v + b) \geq e(v) + b$ , proving the claim.

We now prove that  $e(v) + D \leq e(v + D)$  for all  $v \in \mathbb{Z}$ . This is because  $e(v) + kD = e(v) + b = e(v + b) = e(v + kD) = e(v + D + (k - 1)D) \leq e(v + D) + (k - 1)D$ , the latter inequality holding since  $D$  is the maximal distance in the relation  $E$  and cannot be increased. Subtracting  $(k - 1)D$  on both sides, our claim follows.

Since  $D$  cannot be increased, we have  $e(v + D) \leq e(v) + D$  for all  $v \in \mathbb{Z}$ , and we have proved the lemma. ■

The following lemma summarizes the preceding two lemmas.

**Lemma 8** *The following are equivalent for an endomorphism  $e$  of  $\Gamma$ :*

- (i) *There exists  $k > c + 1$  such that  $d(ex, ey) \geq k$  for all  $x, y \in \mathbb{Z}$  with  $d(x, y) = k$ .*
- (ii)  *$e$  does not generate a finite range operation.*
- (iii)  *$e$  satisfies either  $e(v + D) = e(v) + D$  or  $e(v + D) = e(v) - D$ .*

PROOF: Lemma 7 shows that (i) implies (ii) and (iii). It follows from Lemma 6 that (ii) implies (i). Finally, it is clear that (iii) implies (ii). ■

We know now that there are two types of endomorphisms of  $\Gamma$ : Those which are periodic with period  $D$ , and those which generate a finite range operation. We will now provide examples showing that both types really occur.

**Example 9** *Let  $R := \{(x, y) : d(x, y) = 1 \vee d(x, y) = 3\}$ , and set  $\Gamma := (\mathbb{Z}; R)$ . Set  $e(3k) := 3k$ ,  $e(3k + 1) := 3k + 1$ , and  $e(3k + 2) := 3k$ , for all  $k \in \mathbb{Z}$ . Then  $e$  is an endomorphism of  $\Gamma$  that does not generate any finite range operations since it satisfies  $e(v + 3) = e(v) + 3$  for all  $v \in \mathbb{Z}$ .*

Observe that in the previous example, we checked that  $e$  is of the non-finite-range type by virtue of the easily verifiable Item (iii) of Lemma 8 and without calculating  $c(\Gamma)$ , which would be more complicated.

**Example 10** *For the structure  $\Gamma$  from Example 9, let  $e$  be the function which maps every  $x \in \mathbb{Z}$  to its value modulo 4. Then  $e$  is an endomorphism which has finite range.*

**Example 11** *Set  $R := \{(x, y) : d(x, y) \in \{1, 3, 6\}\}$  and  $S := \{(x, y) : d(x, y) = 3\}$ . Then  $\Gamma := (\mathbb{Z}; R, S)$  has the endomorphism from Example 9. However, it does not have any finite range endomorphism. To see this, consider the set  $\mathbb{Z}_3 := \{3m : m \in \mathbb{Z}\}$ . If  $e$  were a finite range endomorphism, it would have to map this set onto a finite set. Assume wlog that  $e(0) = 0$  and  $e(3) > 0$ . Then  $e(3) = 3$  as  $e$  preserves  $S$ . We claim  $e(s) = s$  for all  $s \in \mathbb{Z}_3$ . Suppose to the contrary that  $s$  is the minimal positive counterexample (the negative case is similar). We have  $e(s - 3) = s - 3$  and hence, as  $e$  preserves  $S$ ,  $e(s) \in \{s - 6, s\}$ . If we had  $e(s) = s - 6$ , then  $e(s - 6) = s - 6$  and  $(s - 6, s) \in R$  yields a contradiction.*

**Example 12** *Let  $\Gamma = (\mathbb{Z}; \text{sym-succ})$ , and let  $e$  be the function that maps every  $x$  to its absolute value. Then  $e$  does not have finite range, but does generate a function with finite range (of size 2).*

The proof of Lemma 7 generalizes canonically to a more general situation.

**Lemma 13** *Let  $e$  be an endomorphism of  $\Gamma$  satisfying the various statements of Lemma 8. Let  $q$  be so that  $d(x, y) = q$  implies that  $d(ex, ey) \leq q$ . Then  $e$  satisfies either  $e(v + q) = e(v) + q$  for all  $v \in \mathbb{Z}$ , or  $e(v + q) = e(v) - q$  for all  $v \in \mathbb{Z}$ .*

PROOF: This is the same argument as in the proof of Lemma 7, with  $D$  replaced by  $q$ . ■

**Definition 14** *Given an endomorphism  $e$  of  $\Gamma$ , we call all positive natural numbers  $q$  with the property that  $e(v + q) = e(v) + q$  for all  $v \in \mathbb{Z}$  or  $e(v + q) = e(v) - q$  for all  $v \in \mathbb{Z}$  stable for  $e$ .*

Observe that if  $e$  satisfies the various statements of Lemma 8, then  $D$  is stable for  $e$ . Note also that if  $p, q$  are stable for  $e$ , then they must have the same “direction”: We cannot have  $e(v + p) = e(v) + p$  and  $e(v + q) = e(v) - q$  for all  $v \in \mathbb{Z}$ .

**Lemma 15** *Let  $e$  satisfy the various statements of Lemma 8, and let  $q$  be the minimal stable number for  $e$ . Then the stable numbers for  $e$  are precisely the multiples of  $q$ . In particular,  $q$  divides  $D$ .*

PROOF: Clearly, all multiples of  $q$  are stable. Now for the other direction suppose that  $p$  is stable but not divisible by  $q$ . Write  $p = m \cdot q + r$ , where  $m, r$  are positive numbers and  $0 < r < q$ . Since  $r$  is not stable, applying  $e$  and shifts we can find a term  $t$  such that  $t(0) = 0$  and  $d(t(mq), t(p)) \neq r$ . By the property of  $p$  we should have  $t(p) = p$ . But this is impossible since then  $d(t(mq), t(p)) = d(mq, p) = r$ , a contradiction. ■

**Lemma 16** *Let  $e$  be an endomorphism of  $\Gamma$  satisfying the statements of Lemma 8. Let  $q$  be its minimal stable number. Then  $e$  can be composed with automorphisms of  $(\mathbb{Z}; \text{succ})$  to obtain an endomorphism  $t$  with the following properties:*

- $t$  satisfies either  $t(v + q) = t(v) + q$  or  $t(v + q) = t(v) - q$
- $t(0) = 0$
- $t[\mathbb{Z}] = \{q \cdot z : z \in \mathbb{Z}\}$ .

PROOF: Assume  $1 < q$  (otherwise  $t$  can be chosen to be the identity and there is nothing to do). We claim that  $e$  generates a term  $t_1$  such that  $t_1(0) = 0$  and  $t_1(1) \in \{q \cdot z : z \in \mathbb{Z}\}$ . To see this, observe that since  $1 < q$  and since  $q$  is the smallest positive number with the property that  $d(x, y) = q$  implies  $d(ex, ey) \leq q$ , there exist  $x_0, y_0 \in \mathbb{Z}$  with  $d(x_0, y_0) = 1$  and  $d(ex_0, ey_0) > 1$ . Write  $r_1 := d(ex_0, ey_0)$ . If  $r_1$  is not a multiple of  $q$ , then there exist  $x_1, y_1 \in \mathbb{Z}$  with  $d(x_1, y_1) = r_1$  and  $d(ex_1, ey_1) =: r_2 > r_1$ . Again, if  $r_2$  is not a multiple of  $q$ , then there exist  $x_2, y_2 \in \mathbb{Z}$  with  $d(x_2, y_2) = r_2$  and  $d(ex_2, ey_2) =: r_3 > r_2$ . Consider the sequence  $(x_i, y_i)$  of pairs of distance  $r_i$  (setting  $r_0 := 1$ ). By exchanging  $x_{i+1}$  and  $y_{i+1}$  if necessary, we may assume that  $x_{i+1} < y_{i+1}$  iff  $ex_i < ey_i$ , for all  $i$ . There exist automorphisms  $\alpha_i$  of  $(\mathbb{Z}; \text{succ})$  such that  $(\alpha_i(e(x_i)), \alpha_i(e(y_i))) = (x_{i+1}, y_{i+1})$ . Set  $s_i := \alpha_i \circ e \circ \alpha_{i-1} \circ \cdots \circ \alpha_0 \circ e$ . Then the endomorphism  $s_i$  sends  $(x_0, y_0)$  to  $(x_{i+1}, y_{i+1})$ , a pair of distance  $r_{i+1} > r_i > \cdots > r_0$ . Thus the sequence must end at some finite  $i$ . By construction of the sequence, this happens only if  $r_{i+1}$  is a multiple of  $q$ . Therefore,  $r_{i+1} = d(s_i(x_0), s_i(y_0)) \in \{q \cdot z : z \in \mathbb{Z}\}$ . By applying shifts we may assume  $x_0 = 0$ ,  $y_0 = 1$ , and  $s_i(0) = 0$ . Set  $t_1 := s_i$ .

Now if  $2 < q$ , then consider the number  $t_1(2)$ . We claim that  $e$  generates a term  $t_2$  such that  $t_2(0) = 0$  and  $t_2(t_1(2))$  is a multiple of  $q$ . If already  $t_1(2)$  is a multiple of  $q$ , then we can choose  $t_2$  to be the identity. Otherwise, we can increase the distance of  $t_1(2)$  from 0 successively by applying



shifts and  $e$  just as before, where we moved away 1 from 0. After a finite number of steps, we arrive at a term  $t_2$  such that  $d(t_2(0), t_2 t_1(2))$  is a multiple of  $q$ . Applying a shift one more time, we may assume that  $t_2(0) = 0$ , and so  $t_2$  has the desired properties.

We continue inductively, constructing for every  $i < q$  a term  $t_i$  such that  $t_i(0) = 0$  and  $t_i \circ \dots \circ t_1(i)$  is a multiple of  $q$ . At the end, we set  $t := t_{q-1} \circ \dots \circ t_1$ . Since  $e$  satisfies either  $e(v + q) = e(v) + q$  or  $e(v + q) = e(v) - q$ , so does  $t$ , as it is composed of  $e$  and automorphisms of  $(\mathbb{Z}; \text{succ})$ . It is also clear from the construction that  $t(0) = 0$  holds. These two facts together imply that  $t[\mathbb{Z}]$  contains the set  $\{q \cdot z : z \in \mathbb{Z}\}$ . For the other inclusion, let  $v \in \mathbb{Z}$  be arbitrary, and write  $v = q \cdot z + r$ , where  $z \in \mathbb{Z}$  and  $0 \leq r < q$ . Then  $t(v) = q \cdot z + t(r)$  or  $t(v) = -q \cdot z + t(r)$ , which is a multiple of  $q$  since  $t(r)$  is a multiple of  $q$  by construction. ■

Observe that we did not need local closure in the preceding lemma.

**Lemma 17** *Let  $e$  be an endomorphism of  $\Gamma$  which is not an automorphism of  $(\mathbb{Z}; \text{sym-succ})$ . Then  $e$  is not injective.*

PROOF: If  $e$  generates a finite range operation then the lemma follows immediately, so assume this is not the case. Then  $e$  has a minimal stable number  $q$ . Since  $e$  is not an automorphism of  $(\mathbb{Z}; \text{sym-succ})$ , we have  $q > 1$ . But then the statement follows from the preceding lemma, since the function  $t$  is not injective. ■

**Lemma 18** *Let  $e$  be an endomorphism of  $\Gamma$  which is not an automorphism of  $(\mathbb{Z}; \text{sym-succ})$  and which does not generate a finite range operation. Then  $e$  is not surjective.*

PROOF: This is a direct consequence of Lemma 16, since being surjective is preserved under composition. ■

PROOF: (of Theorem 2) We prove the first statement. It is a direct consequence of Lemma 17 that the automorphism group of  $\Gamma$  is contained in that of  $(\mathbb{Z}; \text{sym-succ})$ . Since  $\Gamma$  is fo-definable in  $(\mathbb{Z}; \text{succ})$ , its automorphism group contains that of  $(\mathbb{Z}; \text{succ})$ . The statement now follows from the easily verifiable fact that there are no permutation groups properly between the automorphism groups of  $(\mathbb{Z}; \text{succ})$  and  $(\mathbb{Z}; \text{sym-succ})$ .

For the second statement, suppose that  $\Gamma$  has no finite range endomorphism. If all of its endomorphisms are automorphisms, then we are done. Otherwise,  $\Gamma$  has an endomorphism  $t$  as in Lemma 16, with  $q > 1$ . Consider the substructure  $\Delta$  of  $\Gamma$  induced on the image  $t[\mathbb{Z}] = \{q \cdot z : z \in \mathbb{Z}\}$  of  $t$ . We claim that  $\Delta$  is isomorphic to a structure  $\Delta'$  with domain  $\mathbb{Z}$  which has a first-order definition in  $(\mathbb{Z}; \text{succ})$ . Indeed, let  $R$  be any relation of  $\Gamma$ , and let  $\phi$  be the formula defining  $R$  in  $(\mathbb{Z}; \text{succ})$ . For all  $i \in \omega$ , let  $\text{succ}^i$  be the binary relation on  $\mathbb{Z}$  which says about a pair  $(x, y) \in \mathbb{Z}^2$  that  $y = x + i$ . Then adding the  $\text{succ}^i$  to the language,  $\phi$  can be assumed to be quantifier-free. Now construct a formula  $\phi'$  as follows: For all  $i \in \omega$  not divisible by  $q$ , replace every occurrence of  $\text{succ}^i$  by  $\forall x(x \neq x)$ . For all other  $i$ , replace every occurrence of  $\text{succ}^i$  by  $\text{succ}^{\frac{i}{q}}$ . Let  $R'$  be the relation defined by  $\phi'$  on  $\mathbb{Z}$ . Then one readily checks that  $(t[\mathbb{Z}], R)$  (where  $R$  is restricted to the domain  $t[\mathbb{Z}]$ ) is isomorphic to  $(\mathbb{Z}; R')$  via the isomorphism which sends every  $x \in t[\mathbb{Z}]$  to  $\frac{x}{q}$ . Thus, defining  $\Delta'$  to have exactly the relations of the form  $R'$ , where  $R$  is a relation of  $\Gamma$ , we get that  $\Delta'$  is indeed isomorphic to  $\Delta$ . Clearly,  $\Delta'$  is fo-definable in  $(\mathbb{Z}; \text{succ})$ .

Since  $\Delta$  is the image of an endomorphism of  $\Gamma$ , one readily checks that the Gaifman graph of  $\Delta$  coincides with the induced subgraph of the Gaifman graph of  $\Gamma$  on  $t[\mathbb{Z}]$ . Thus in  $\Delta$ , two points  $x, y$  are adjacent iff  $d(x, y) \in \{d_1, \dots, d_n\}$ ; moreover,  $d(x, y)$  is divisible by  $q$ . Therefore, the remaining

relevant distances are those divisible by  $q$ . In other words, if  $\{d_{i_1}, \dots, d_{i_r}\}$  are those distances from  $\{d_1, \dots, d_n\}$  which are divisible by  $q$ , then the Gaifman graph of  $\Delta'$  is isomorphic to the graph on  $\mathbb{Z}$  defined by the distances  $\{\frac{d_{i_1}}{q}, \dots, \frac{d_{i_r}}{q}\}$ . Since before, the greatest common divisor of all possible distances was 1, we must have lost at least one distance, i.e.,  $r < n$ .

Observe that  $\Delta$  (and hence  $\Delta'$ ) is connected as it is the image of an endomorphism of  $\Gamma$ . Note moreover that  $\Delta$  cannot have a finite range endomorphism: If  $s$  were such an endomorphism, then  $s \circ t$  would be a finite range endomorphism for  $\Gamma$ , contrary to our assumption. If all endomorphisms of  $\Delta$  are automorphisms, then we are done. Otherwise  $\Delta$  (more precisely,  $\Delta'$ ) satisfies all assumptions that we had on  $\Gamma$ , and we may repeat the argument. Since in every step we lose a distance for the Gaifman graph, this process must end, meaning that we arrive at a structure all of whose endomorphisms are automorphisms. ■

## 4 Definability of Successor

In this section we show how to reduce the complexity classification for distance constraint satisfaction problems with template  $\Gamma$  to the case where either  $\Gamma$  has a finite core, or the relation  $\text{succ}$  is pp-definable in  $\Gamma$ . We make essential use of the results of the previous section; but note that in this section we do *not* assume that  $\Gamma$  is connected.

**Theorem 19** *Every finite degree relational structure  $\Gamma$  with a first-order definition in  $(\mathbb{Z}; \text{succ})$  is either homomorphically equivalent to a finite structure, or to a connected finite-degree structure  $\Delta$  with a first order definition in  $(\mathbb{Z}; \text{succ})$  which satisfies one of two possibilities:  $\text{CSP}(\Delta)$  (and, hence,  $\text{CSP}(\Gamma)$ ) is NP-hard, or  $\text{succ}$  is definable in  $\Delta$ .*

The following lemma demonstrates how the not necessarily connected case can be reduced to the connected case.

**Lemma 20** *Every finite degree relational structure  $\Gamma$  with a first-order definition in  $(\mathbb{Z}; \text{succ})$  is homomorphically equivalent to a connected finite-degree structure  $\Delta$  with a first order definition in  $(\mathbb{Z}; \text{succ})$ .*

PROOF: If the Gaifman graph of  $\Gamma$  does not contain any edges, then the statement is clear. Otherwise, let  $g$  be the greatest common divisor of  $d_1, \dots, d_n$  (the *distances* in the Gaifman graph, see Section 3, Definition 3). If  $\Gamma$  is connected, there is nothing to prove.

Otherwise, if  $\Gamma$  is disconnected, we have  $g > 1$ . Then  $\Gamma$  must be a disjoint union of  $g$  copies of a connected structure  $\Delta$  (and these copies are isomorphic to each other by an isomorphism of the form  $x \mapsto x + d$ , for appropriate constant  $d$ ). In particular,  $\Gamma$  is homomorphically equivalent to  $\Delta$ . Moreover, we claim that  $\Delta$  itself has a first-order definition in  $(\mathbb{Z}; \text{succ})$ . The proof here is as in the proof of Theorem 2, with  $g$  taking the role of  $q$ . ■

The following is obvious.

**Lemma 21** *Let  $(a_1, \dots, a_k), (b_1, \dots, b_k) \in \mathbb{Z}^k$ . Then there is an automorphism  $\alpha$  of  $(\mathbb{Z}; \text{succ})$  with  $\alpha(a_i) = b_i$  for all  $i \leq k$  if and only if  $a_i - a_j = b_i - b_j$  for all  $1 \leq i, j \leq k$ .*

**Lemma 22** *Suppose that  $\Gamma$  is connected. Then there is an  $n_0$  such that  $\Gamma[\{1, \dots, n\}]$  is connected for all  $n \geq n_0$ .*

PROOF: Let  $d_1$  be the smallest distance of the distances  $\{d_1, \dots, d_n\}$  defining the Gaifman graph  $G$  of  $\Gamma$  (as in Section 3). By connectivity of  $G$ , for each pair  $a, b$  of elements from  $\{1, \dots, d_1\}$  there is a path from  $a$  to  $b$  in  $G$ . Fix such a path for each pair  $a, b$ . Let  $n_0$  be the smallest number such that all vertices on those paths are smaller than  $n_0$ . We claim that  $\Gamma[\{1, \dots, n\}]$  is connected for all  $n \geq n_0$ . To see that  $c, d \leq n$  are connected, observe that both  $c$  and  $d$  are connected to vertices in  $\{1, \dots, d_1\}$  (via a sequence of vertices at distance  $d_1$ ). Since all vertices in  $\{1, \dots, d_1\}$  are connected in  $\Gamma[\{1, \dots, n_0\}]$  by construction, we conclude that  $c$  and  $d$  are connected by a path in  $\Gamma[\{1, \dots, n\}]$ . ■

**Lemma 23** *Suppose that  $\Gamma$  is connected and of finite degree. Then there is an  $n_0$  and  $c$  such that for all  $n \geq n_0$  and any homomorphism  $f$  from  $\Gamma[\{1, \dots, n\}]$  to  $\Gamma$  we have that  $d(f(x), f(y)) \leq c + d(x, y)$  for all  $x, y \in \{1, \dots, n\}$ .*

PROOF: Let  $n_0$  be the number from Lemma 22. Then for all  $n \geq n_0$ , the structure  $\Gamma[\{1, \dots, n\}]$  is connected. Now, proceed as in Lemma 5. ■

**Proposition 24** *Let  $\Gamma$  be a connected finite-degree structure with a first-order definition in  $(\mathbb{Z}; \text{succ})$ . Assume that every endomorphism of  $\Gamma$  is an automorphism of  $(\mathbb{Z}; \text{sym-succ})$ . Then for all  $a_1, a_2 \in \mathbb{Z}$  there is a finite  $S \subseteq \mathbb{Z}$  that contains  $\{a_1, a_2\}$  such that for all homomorphisms  $f$  from  $\Gamma[S]$  to  $\Gamma$  we have  $d(f(a_1), f(a_2)) = d(a_1, a_2)$ .*

PROOF: Suppose that there are  $a_1 < a_2 \in \Gamma$  such that for all finite subsets  $S$  of elements of  $\Gamma$  that contain  $\{a_1, a_2\}$  there is a homomorphism from  $\Gamma[S]$  to  $\Gamma$  where  $d(f(a_1), f(a_2)) \neq d(a_1, a_2)$ . We have to show that  $\Gamma$  has an endomorphism that is not an automorphism of  $(\mathbb{Z}; \text{sym-succ})$ . Let  $S$  be a subset of  $\mathbb{Z}$  that contains  $\{a_1, a_2\}$ , and let  $f, g$  be functions from  $S \rightarrow \mathbb{Z}$ . Then we define  $f \sim g$  if there exists an automorphism  $\alpha$  of  $\Gamma$  such that  $f(x) = \alpha(g(x))$  for all  $x \in S$ . We call such a function *good* if it is a homomorphism from  $\Gamma[S]$  to  $\Gamma$  where  $d(f(a_1), f(a_2)) \neq d(a_1, a_2)$ . Observe that since all automorphisms of  $\Gamma$  preserve distances, if one function in an equivalence class is good, then all other functions in the equivalence class are also good.

Let  $n_0$  be the number from Lemma 23, and let  $n_1$  be  $\max(n_0, |a_1|, |a_2|)$ . Consider the following infinite forest  $\mathcal{T}$ : the vertices are the equivalence classes of good functions  $f : V \rightarrow \mathbb{Z}$  for  $V = \{-n, \dots, n\}$ , for all  $n \geq n_1$ , and  $\mathcal{T}$  has an arc from one such equivalence class  $F$  to another  $H$  if there are  $f \in F, h \in H$ , such that  $f$  is a restriction of  $h$ , and  $f$  is defined on  $\{-n, \dots, n\}$ , and  $h$  is defined on  $\{-n-1, \dots, n+1\}$ , for some  $n \in \mathbb{N}$ . Observe that

- by our assumptions the forest  $\mathcal{T}$  is infinite;
- by Lemma 23, for every  $n \geq n_1$  there is a  $b$  such that  $d(f(x), f(y)) < b$  for all  $x, y \in \{-n, \dots, n\}$ . Using Lemma 21 it follows that  $\mathcal{T}$  is finitely branching;
- the forest  $\mathcal{T}$  has only finitely many roots.

By König's tree lemma, there is an infinite branch in  $\mathcal{T}$ . It is straightforward to use this infinite branch to construct an endomorphism  $f$  of  $\Gamma$  with  $d(a_1, a_2) \neq d(f(a_1), f(a_2))$ . This endomorphism cannot be an automorphism of  $(\mathbb{Z}; \text{sym-succ})$ , which concludes the proof. ■

**Corollary 25** *Suppose that  $\Gamma$  is a connected finite-degree structure with a first-order definition in  $(\mathbb{Z}; \text{succ})$ , and suppose that all endomorphisms of  $\Gamma$  are automorphisms of  $\Gamma$ . Then either the relation  $\text{sym-succ}^k = \{(x, y) \mid d(x, y) = k\}$  is pp-definable in  $\Gamma$  for every  $k \geq 1$ , or the relation  $\text{succ}^k = \{(x, y) \mid x - y = k\}$  is pp-definable in  $\Gamma$  for every  $k \geq 1$ .*

PROOF: First consider the case that  $\Gamma$  is preserved by the unary operation  $x \mapsto -x$ , and let  $k \geq 1$  be arbitrary. Let  $a_1, a_2$  be any two elements of  $\mathbb{Z}$  at distance  $k$ . Since all endomorphisms of  $\Gamma$  are automorphisms of  $\Gamma$ , they are automorphisms of  $(\mathbb{Z}; \text{sym-succ})$  by the first statement of Theorem 2. Hence we may apply Proposition 24, and there is a finite set  $S \subseteq \mathbb{Z}$  such that every homomorphism  $f$  from  $\Gamma[S]$  to  $\Gamma$  satisfies  $d(f(a_1), f(a_2)) = d(a_1, a_2)$ . Let  $\phi(a_1, a_2)$  be the primitive positive formula obtained from the canonical query for  $\Gamma[S]$  by existentially quantifying all vertices except for  $a_1$  and  $a_2$ . We claim that  $\phi$  is a pp-definition of  $\text{sym-succ}^k = \{(x, y) \mid d(x, y) = k\}$ .

The relation defined by  $\phi$  contains the pair  $(a_1, a_2)$  (since the identity mapping is a satisfying assignment for the canonical query  $\Gamma[S]$ ), and since  $\Gamma$  is preserved by all automorphisms of  $(\mathbb{Z}; \text{sym-succ})$  it also contains all other pairs  $(x, y) \in \mathbb{Z}^2$  such that  $d(x, y) = k = d(a_1, a_2)$ . Conversely,  $\phi$  does not contain any pair  $(x, y)$  with  $d(x, y) \neq k$ . Otherwise, there must be a assignment  $f : S \rightarrow \mathbb{Z}$  that satisfies the canonical query and maps  $a_1$  to  $x$  and  $a_2$  to  $y$ . This assignment is a homomorphism, and therefore contradicts the assumption that  $d(f(a_1), f(a_2)) = d(a_1, a_2)$ . This proves the claim.

Now consider the case that  $\Gamma$  is *not* preserved by the unary operation  $-$ . As before we use Theorem 2 and Proposition 24 to construct a primitive positive formula  $\phi$ . This time it is easy to see that  $\phi$  defines the relation  $\{(x, y) \mid x - y = k\}$ . ■

**Proposition 26** *Suppose that for all  $k$  the relation  $\text{sym-succ}^k = \{(x, y) \in \mathbb{Z}^2 \mid d(x, y) = k\}$  is pp-definable in  $\Gamma$ . Then  $\text{CSP}(\Gamma)$  is NP-hard.*

PROOF: Observe that the primitive positive formula  $\exists y. d(x, y) = 1 \wedge d(y, z) = 5$  defines the relation  $R = \{(x, z) \mid d(x, z) \in \{4, 6\}\}$ . The structure  $(\mathbb{Z}; R)$  decomposes into two copies of the structure  $(\mathbb{Z}; S)$  where  $S = \{(x, y) \mid d(x, y) \in \{2, 3\}\}$ . This structure has the endomorphism  $x \mapsto x \bmod 5$ , and the image induced by this endomorphism is a cycle of length 5, which has a hard CSP (this is well-known; for a much stronger result on undirected graphs, see Hell and Nešetřil [14]). ■

PROOF: (of Theorem 19) By Lemma 20, we can assume without loss of generality that  $\Gamma$  is connected. Clearly, if  $\Gamma$  has a finite range endomorphism, then it has a finite core. Otherwise, by Theorem 2, there is an endomorphism of  $\Gamma$  that maps  $\Gamma$  onto a subset of  $\mathbb{Z}$  isomorphic to an induced substructure  $\Delta$  of  $\Gamma$  which is first-order definable in  $(\mathbb{Z}; \text{succ})$ , and where all endomorphisms are automorphisms. Being the homomorphic image of the connected structure  $\Gamma$ ,  $\Delta$  must also be connected. We now apply Corollary 25 to  $\Delta$ . If the relation  $\{(x, y) \mid d(x, y) = k\}$  is pp-definable in  $\Delta$  for every  $k \geq 1$ , then  $\text{CSP}(\Gamma)$  (which is equal to  $\text{CSP}(\Delta)$  since  $\Gamma$  and  $\Delta$  are homomorphically equivalent) is NP-hard by Proposition 26. Otherwise, by Corollary 25, the relation  $\{(x, y) \mid x - y = k\}$ , and in particular the relation  $\text{succ}$  is pp-definable in  $\Delta$ . ■

## 5 The Power of Consistency

All tractable distance constraint satisfaction problems for templates without a finite core can be solved by an algorithmic technique known as *local consistency*. We prove these tractability results in this section.

A *majority operation* on a set  $X$  is a mapping  $f : X^3 \rightarrow X$  satisfying

$$f(x, x, y) = f(x, y, x) = f(y, x, x) = x.$$

An  $n$ -ary relation  $R$  on a set  $X$  is *2-decomposable* if  $R$  contains all  $n$ -tuples  $(t_1, \dots, t_n)$  such that for every 2-element subset  $I$  of  $\{1, \dots, n\}$  there is a tuple  $s \in R$  such that  $t_i = s_i$  for all  $i \in I$ .

We need the following concept to prove the algorithmic results in this paper. Let  $\Delta$  be a structure with a (not necessarily finite) relational signature  $\tau$ , and let  $\phi$  be a conjunction of atomic  $\tau$ -formulas with variables  $V$ . For  $k > 0$ , we say that  $\phi$  is *k-consistent* (with respect to  $\Delta$ ) if for every assignment  $\alpha$  of  $k - 1$  variables  $x_1, \dots, x_{k-1} \in V$  to elements from  $\Delta$  and for every variable  $x_k \in V$  the assignment  $\alpha$  can be extended to  $x_k$  such that all conjuncts of  $\phi$  that involve no other variables than  $x_1, \dots, x_k$  are satisfied over  $\Delta$  by the extension of  $\alpha$ . We say that  $\phi$  is *strongly k-consistent* if  $\phi$  is *j-consistent* for all  $j$  with  $2 \leq j \leq k$ . We say that  $\phi$  is *globally consistent* if  $\phi$  is *k-consistent* for all  $k > 0$ .

The following has been shown in [17] (with an explicit comment in Section 4.4 that the result also holds on infinite domains).

**Theorem 27 (Special case of Theorem 3.5 of [17])** *Let  $\Gamma$  be a structure with a majority polymorphism. Then every relation  $R$  of  $\Gamma$  is 2-decomposable. Moreover, every strongly 3-consistent conjunction of atomic formulas is also globally consistent with respect to  $\Gamma$ .*

In the proof of the following proposition, and in the next section, it will be convenient to represent binary relations  $R \subseteq \mathbb{Z}^2$  with a first-order definition in  $(\mathbb{Z}; \text{succ})$  by sets of integers as follows: the set  $S$  represents the binary relation  $R_S := \{(x, x+k) \mid k \in S\}$ . Conversely, when  $R$  is a binary relation with a first-order definition in  $(\mathbb{Z}; \text{succ})$ , let  $S(R)$  be the set such that  $R_{S(R)} = R$ . It is easy to see that every binary relation of finite degree and with a first-order definition in  $(\mathbb{Z}; \text{succ})$  is of the form  $R_S$  for some finite  $S$ .

**Theorem 28** *Let  $\Gamma$  be a finite degree structure with a first-order definition in  $(\mathbb{Z}; \text{succ})$ . If  $\Gamma$  has a majority polymorphism, then  $\text{CSP}(\Gamma)$  is in  $P$ .*

PROOF: Let  $D$  be the largest distance in the Gaifman graph of  $\Gamma$ , as in Section 3 (Definition 3). Let  $\Phi$  be an input instance to  $\text{CSP}(\Gamma)$  with variables  $V = \{x_1, \dots, x_n\}$ , and let  $\phi$  be the quantifier-free part of  $\Phi$ . Our algorithm and its correctness proof work independently for each connected component of the canonical database of  $\phi$ . So let us assume that the canonical database of  $\phi$  is connected.

Let  $\Delta$  be the expansion of  $\Gamma$  by all binary relations  $R$  with a pp-definition in  $\Gamma$  such that  $R = R_S$  for  $S \subseteq \{-nD, \dots, nD\}$ . Moreover,  $\Delta$  contains a binary relation symbol  $F$  that denotes  $R_{\mathbb{Z}} = \mathbb{Z}^2$ . Let  $\tau$  be the signature of  $\Delta$ . Since all relations of  $\Delta$  are pp-definable in  $\Gamma$ , it follows that  $\Delta$  has the same majority polymorphism as  $\Gamma$ .

We claim that we can compute from  $\phi$  a  $\tau$ -formula  $\psi$  with variables  $V$  such that

- $\phi$  implies  $\psi$ , and
- $\phi \wedge \psi$  is strongly 3-consistent with respect to  $\Delta$

in time polynomial in the size of  $\phi$ . This can be done as follows.

The algorithm maintains for each pair of variables  $x_k, x_l$  with  $k, l \in \{1, \dots, n\}$  and  $k \neq l$  a binary relation symbol  $P = P^{(k,l)}$  from  $\tau$ . The set  $S(P^\Delta)$  either equals  $\mathbb{Z}$  or it is a subset of  $\{-nD, \dots, nD\}$ ; in the latter case, we use this subset to represent the relation in the algorithm.

We first describe how to initialize the  $P^{(k,l)}$ . Let  $k, l \in \{1, \dots, n\}$  be distinct. If  $x_k$  and  $x_l$  are non-adjacent in the Gaifman graph of the canonical query for  $\phi$ , then we set  $P^{(k,l)}$  to  $F$ . Otherwise, there is a conjunct  $T(x_{i_1}, \dots, x_{i_m})$  of  $\phi$  with  $T$  a relation symbol from  $\Gamma$  such that  $k, l \in \{i_1, \dots, i_m\}$ . For the sake of notation, suppose that  $i_j = j$  for all  $1 \leq j \leq m$ , and that  $k = 1$  and  $l = 2$ . Let  $R(x_1, x_2)$  be the relation with the pp-definition  $\exists x_3, \dots, x_m. T(x_1, \dots, x_m)$  over  $\Gamma$ .

Clearly,  $S(R) \subseteq \{-D, \dots, D\}$ . Hence,  $R$  is a relation from  $\Delta$ . We then set  $P^{(k,l)}$  to  $R$ . Note that  $R(x_1, x_2)$  is implied by  $\phi$  in  $\Delta$ .

We now describe how to obtain stronger and stronger consequences of  $\phi$  by local propagation. Let  $x_k, x_l, x_m$  be three distinct variables from  $\phi$ . Consider the case  $k = 1, l = 2$ , and  $m = 3$ , again for the sake of notation. Then let  $R(x_1, x_3)$  be the binary relation defined by  $\exists x_2. P^{(1,3)}(x_1, x_3) \wedge P^{(1,2)}(x_1, x_2) \wedge P^{(2,3)}(x_2, x_3)$  over  $\Delta$ . It is straightforward to verify that  $R$  is pp-definable in  $\Gamma$ . We will show below that either  $S(R) \subseteq \{-nD, \dots, nD\}$  or  $S(R) = \mathbb{Z}$ . Hence,  $R$  is a relation from  $\Delta$  and we replace  $P^{(1,3)}$  by  $R$ . We call this replacement step *proper* if  $R$  was different from  $P^{(1,3)}$ . Again, note that  $R(x_1, x_3)$  is implied by  $\phi$  in  $\Delta$ . Also note that a representation of  $R$  can be computed from the representations of  $P^{(1,2)}$ ,  $P^{(2,3)}$ , and  $P^{(1,3)}$  in polynomial time. Moreover,  $S(R) \subseteq S(P^{(1,3)})$ .

We perform such replacements until for each  $k, l$  the binary relation  $P^{(k,l)}$  cannot be changed further by the above replacement steps. It is clear that we will reach this state after an at most cubic number of proper replacement steps: the reason is that when a relation that is represented by a subset  $S$  of  $\{-nD, \dots, nD\}$  is replaced, the representation of the replacing relation will be a proper subset of  $S$ . Since there are only quadratically many relations where replacements can be made, the claim follows.

We still have to show that  $S(R) \subseteq \{-nD, \dots, nD\}$  or  $S(R) = \mathbb{Z}$  for  $R(x_1, x_3)$  defined by  $\exists x_2. P^{(1,3)}(x_1, x_3) \wedge P^{(1,2)}(x_1, x_2) \wedge P^{(2,3)}(x_2, x_3)$  as above. The proof is by induction on the distance  $l$  of  $x_1$  and  $x_3$  in the Gaifman graph  $G$  of the canonical database of  $\phi$ ; in fact, we show the stronger claim that either  $S(R) = \mathbb{Z}$  or  $S(R) \subseteq \{-lD, \dots, lD\}$ . If the distance is 1, then already by the initialization we have that  $S(P^{(1,3)}) \subseteq \{-D, \dots, D\}$ , and hence  $S(R) \subseteq \{-D, \dots, D\}$ . If  $S(P^{(1,3)}) \subseteq \{-lD, \dots, lD\}$ , then  $R \subseteq \{-lD, \dots, lD\}$  and we are done; so assume that  $S(P^{(1,3)}) = \mathbb{Z}$ . Let  $l_1$  be the distance between  $x_1$  and  $x_2$ , and  $l_2$  be the distance between  $x_2$  and  $x_3$  in  $G$ . If  $S(P^{(1,2)}) = \mathbb{Z}$  or  $S(P^{(2,3)}) = \mathbb{Z}$  then  $S(R) = \mathbb{Z}$  and we are done. Otherwise, by inductive assumption we have that  $S(P^{(1,2)}) \subseteq \{-l_1D, \dots, l_1D\}$  and  $S(P^{(2,3)}) \subseteq \{-l_2D, \dots, l_2D\}$ , and because  $l \leq l_1 + l_2$  it follows that  $S(R) \subseteq \{-lD, \dots, lD\}$ .

To conclude the proof, let  $\psi$  be the formula  $\bigwedge_{k,l \in \{1, \dots, n\}, k \neq l} P^{(k,l)}(x_k, x_l)$ . It is straightforward to verify that  $\phi \wedge \psi$  is 3-consistent with respect to  $\Delta$ . Clearly, it is also 2-consistent. Since  $\Delta$  has a majority polymorphism, Theorem 27 implies that  $\phi \wedge \psi$  is globally consistent.

When  $P^{(k,l)} = \emptyset$  for some  $k, l$  then  $\psi$  is unsatisfiable in  $\Delta$ ; and  $\Phi$  is false in  $\Gamma$ . Otherwise, global consistency implies that the sentence  $\exists x_1, \dots, x_n. \phi \wedge \psi$  is true in  $\Delta$ , since we can map  $x_1$  to an arbitrary value in  $\mathbb{Z}$ , and then successively extend this map to a mapping that satisfies  $\phi \wedge \psi$ . It is clear that in this case  $\Phi$  is true in  $\Gamma$  as well. This shows that truth of a given formula  $\Phi$  in  $\Gamma$  can be decided in polynomial time.  $\blacksquare$

**Definition 29** *The  $d$ -modular median is the ternary operation  $m_d : \mathbb{Z}^3 \rightarrow \mathbb{Z}$  defined as follows:*

- *If  $x, y, z$  are congruent modulo  $d$ , then  $m_d(x, y, z)$  equals the median of  $x, y, z$ .*
- *If precisely two arguments from  $x, y, z$  are congruent modulo  $d$  then  $m_d(x, y, z)$  equals the first of those arguments in the ordered sequence  $(x, y, z)$ .*
- *Otherwise,  $m_d(x, y, z) = x$ .*

Clearly,  $d$ -modular median operations are majority operations.

**Corollary 30** *Let  $\Gamma$  be a finite-degree structure with a first-order definition in  $(\mathbb{Z}; \text{succ})$  and a finite relational signature, and suppose that  $\Gamma$  has a modular median polymorphism. Then  $\text{CSP}(\Gamma)$  is in  $P$ .*

## 6 Classification

In this section we finish the complexity classification for those  $\Gamma$  that do not have a finite core. The main result of Section 4 shows that, unless  $\Gamma$  has a finite core, for the complexity classification of  $\text{CSP}(\Gamma)$  we can assume that the structure  $\Gamma$  contains the relation *succ*. In the following we therefore assume that the structure  $\Gamma$  contains the relation *succ*; moreover, we freely use expressions of the form  $x - y = d$ , for fixed  $d$ , in primitive positive definitions since such expressions have themselves pp-definitions from *succ* and therefore from  $\Gamma$ . Our main result will be the following.

**Theorem 31** *Let  $\Gamma$  be a first-order expansion of  $(\mathbb{Z}; \text{succ})$ . Then  $\Gamma$  is preserved by a modular median and  $\text{CSP}(\Gamma)$  is in  $P$ , or  $\text{CSP}(\Gamma)$  is NP-hard.*

A *d*-progression is a subset of  $\mathbb{Z}$  of the form  $\{k, k + d, \dots, k + ld\}$ , for some  $k, l \in \mathbb{Z}$ . We shall denote  $\{k, k + d, \dots, k + ld\}$  by  $[k, k + ld]_d$ .

**Proposition 32** *Let  $R \subseteq \mathbb{Z}^2$  be a finite-degree binary relation with a first-order definition in  $(\mathbb{Z}; \text{succ})$ . Then the following are equivalent.*

1.  *$R$  is preserved by the  $d$ -modular median  $m_d$ ;*
2.  *$R = R_S$  for a  $d$ -progression  $S$ .*

PROOF: (1  $\Rightarrow$  2). If  $S$  is not a  $d$ -progression then there exist some  $a < b \in S$  such that  $x \notin S$  for all  $a < x < b$  and  $b - a \neq d$ . If  $a - b$  is not multiple of  $d$  then fix  $v$  to be any integer smaller than  $\min(S)$ , otherwise fix  $v$  to be  $a + d$ . Let  $u$  be such that  $(u, v) \in R_S$ . If we apply  $m_d$  to  $(u, v), (0, a), (0, b)$  we obtain  $(0, v)$  which does not belong to  $R_S$ .

(2  $\Rightarrow$  1). Let  $(x_i, y_i), i = 1, 2, 3$  be arbitrary tuples of  $R_S$ . For every  $i, j \in \{1, 2, 3\}$ ,  $x_i - x_j = y_i - y_j \pmod d$ . This implies that if a rule of the Definition 29 is applied to the  $x_i$ 's then the same rule is applied to the  $y_i$ 's. Then we only need to care about the first rule since the other two act as a projection. Let  $(x_a, y_b)$  be the result of applying the median to  $(x_i, y_i), i = 1, 2, 3$  and let  $m$  (resp.  $M$ ) be the minimum (resp. maximum) integer  $n$  such that  $(x_a, n) \in R_S$ . Since  $S$  is a  $d$ -progression,  $(x_a, y_b)$  belongs to  $R_S$  if  $y_b - y_a = 0 \pmod d$  and  $m \leq y_b \leq M$ . The first condition follows from the fact that we apply the first rule. The second condition is shown as follows. By the definition of median there is some  $l \in \{1, 2, 3\}$ ,  $l \neq a$ , such that  $x_l \geq x_a$ . Hence we have that  $y_l$  and  $y_a$  are at least  $m$ , which implies that the median of the second coordinates,  $y_b$ , also is. A symmetric argument shows that  $y_b \leq M$ . ■

**Proposition 33** *Let  $a, b$  be two odd numbers such that  $a < b$ . Then  $\text{CSP}(\mathbb{Z}; \text{succ}, R_{\{0, a, b, a+b\}})$  is NP-hard.*

PROOF: Let  $k$  be the integer  $\frac{a+b}{2}$ . Note that the primitive positive formula

$$\phi(x, z) = \exists y. R_{\{0, a, b, a+b\}}(x, y) \wedge y - z = k$$

defines the relation  $C := \{(x, z) \mid d(x, z) \in \{\frac{b-a}{2}, \frac{b+a}{2}\}\}$ . Consider the mapping  $f : \mathbb{Z} \rightarrow \{0, \dots, b-1\}$  defined by  $f(x) = x \pmod b$ . It follows from  $\frac{b-a}{2} = -\frac{b+a}{2} \pmod b$  that  $f$  is an endomorphism of  $C$ . It also follows by the same reason that the restriction,  $\bar{D}$ , of  $C$  to  $\{0, \dots, b-1\}$  is a graph where every node has two edges. Furthermore if  $m$  is  $\gcd(\frac{b-a}{2}, \frac{b+a}{2})$  then  $D$  is the disjoint union of  $m$  cycles of  $\frac{b}{m}$  nodes. Since  $\frac{b}{m}$  is odd we have that  $\text{CSP}(\mathbb{Z}; C)$  is NP-hard (this follows from [14]). ■

**Lemma 34** *Let  $a, b, c \in \mathbb{Z}$  with  $b \neq c$ . Then  $\text{CSP}(\mathbb{Z}; \text{succ}, R_{\{a,b\}}, R_{\{a,c\}})$  is NP-hard.*

PROOF: First observe that the formula  $\exists u. R_{\{a,b\}}(x, u) \wedge u = y + a$  pp-defines the relation  $R_{\{0,b-a\}}$ ; similarly, there is a pp-definition of  $R_{\{0,c-a\}}$  in  $\Gamma$ . Let  $d = b - a$  and  $e = c - a$ ; we will show that  $\text{CSP}(\mathbb{Z}; \text{succ}, R_{\{0,d\}}, R_{\{0,e\}})$  is NP-hard.

The relation defined by  $\exists u, v. R_{\{0,d\}}(x, u) \wedge R_{\{0,e\}}(u, v)$  is  $R_{\{0,d,e,d+e\}}$ . If both  $d$  and  $e$  are odd, we obtain hardness of the CSP from the previous proposition applied to  $(\mathbb{Z}; \text{succ}, R_{\{0,d,e,d+e\}})$ . If both  $d$  and  $e$  are even, then the structure  $\Delta := (\mathbb{Z}; R_{\{0,d\}}, R_{\{0,e\}}, \{(x, y) \mid x - y = 2\})$  is pp-definable in  $\Gamma$ . The structure  $\Delta$  is isomorphic to the disjoint union of two copies of the structure  $(\mathbb{Z}; \text{succ}, R_{\{0,d/2\}}, R_{\{0,e/2\}})$ ; the claim now follows by induction on  $e$ .

Finally, assume that precisely one of  $d$  or  $e$  is even; say  $d$  is even. Set  $u := \text{lcm}(d, e)/d$  and  $v := \text{lcm}(d, e)/e$ . The formula

$$\begin{aligned} \exists y_1, \dots, y_u, z_1, \dots, z_v. R_{\{0,d\}}(p, y_1) \wedge R_{\{0,d\}}(y_1, y_2) \wedge \dots \wedge R_{\{0,d\}}(y_{u-1}, y_u) \wedge R_{\{0,d\}}(y_u, q) \\ \wedge R_{\{0,e\}}(p, z_1) \wedge R_{\{0,e\}}(z_1, z_2) \wedge \dots \wedge R_{\{0,e\}}(z_{v-1}, z_v) \wedge R_{\{0,e\}}(z_v, q) \end{aligned}$$

with free variables  $p$  and  $q$  defines  $R_{\{0, \text{lcm}(d, e)\}}$ .

We are now again in the case that we can pp-define two relations  $R_{\{0,g\}}$  and  $R_{\{0,h\}}$  for even  $g, h$  (namely,  $g = d$  and  $h = \text{lcm}(d, e)$ ), and thus we are done.  $\blacksquare$

**Lemma 35** *Let  $S$  be a finite set of integers with  $|S| > 1$  and let  $d$  be the greatest common divisor of all  $a - a'$  with  $a, a' \in S$ . Assume (this assumption is only for ease of notation) that all elements of  $S$  are of the form  $i \cdot d$  where  $i \in \mathbb{Z}$ . Let  $m = \min(S)$ ,  $M = \max(S)$ , let  $[jd, kd]_d$  be a maximal  $d$ -progression in  $S$ , let  $l$  be such that  $l \geq \max(j - m - 1, M - k - 1, 0)$  and such that  $k \geq j + l$ . Then every  $d$ -progression with  $r = k - j - l + 1$  elements is pp-definable in  $(\mathbb{Z}; \text{succ}, R_S)$ .*

PROOF: For every  $0 \leq i \leq l$ , let  $R_i(x, y)$  be the pp-formula  $\exists z. (z = x + id) \wedge R_S(z, y)$  which can be built using  $R_S$  and  $\text{succ}$ . Finally let  $R_T$  be the relation defined by  $\bigwedge_{0 \leq i \leq l} R_i(x, y)$ . We claim that  $T$  is precisely  $[(j + l)d, kd]_d$ .

We have  $T \subseteq S$  because the formula contains  $R_0(x, y)$ . Let  $x = nd$  be any element of  $S$ . Let us do a case analysis.

1. Case  $m \leq n < j - 1$ . The smallest  $y$  such that  $R_{j-m-1}(0, y)$  holds is  $(j - 1)d$ . Hence in this case  $x \notin T$ .
2. Case  $j - 1 \leq n < j + l$ . By the maximality of  $[jd, kd]_d$  it follows that  $(j - 1)d \notin S$ . Henceforth we have that  $R_i(0, nd)$  does not hold if we pick  $i = n - j + 1$ . Hence  $x \notin T$ .
3. Case  $j + l \leq n \leq k$ . For every  $1 \leq i \leq l$ , we have that  $R_i(0, x)$  holds as  $j + i \leq n \leq k + i$ . This implies that  $x \in T$ .
4. Case  $k < n \leq M$ . By the maximality of  $[jd, kd]_d$  we have that  $(k + 1)d \notin S$ . Hence by choosing  $i = n - (k + 1)$  we have that  $R_i(0, x)$  does not hold. Consequently  $x \notin T$ .

Finally, it is obvious that if  $T$  is a  $d$ -progression with  $r$  elements, then  $R_T$  can be defined by the pp-formula  $\exists z. (z = x + p) \wedge R_{[(j+l)d, kd]_d}(z, y)$  by choosing  $p = \max(T) - kd$ .  $\blacksquare$

Let us illustrate the construction of  $R_T$  in the previous proof with an example. Assume  $S$  is the set  $\{1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 20\}$  which we can represent as:

$$S \mid \begin{array}{cccccccccccccccccccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 \end{array} \mid$$



We have  $d = 1$ . Consider the 1-progression  $[7, 16]_1$  in  $S$ . Then we have  $m = 1$ ,  $M = 20$ ,  $j = 7$ , and  $k = 16$ . Fix  $l = 6$ . For every  $0 \leq i \leq l$  let  $Z_i$  such that  $R_{Z_i} = R_i$ . Then we have:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
$Z_0$	•																									
$Z_1$		•																								
$Z_2$			•																							
$Z_3$				•																						
$Z_4$					•																					
$Z_5$						•																				
$Z_6$							•																			
$T$																										
	Case 1								Case 2								Case 3								Case 4	

**Lemma 36** *Let  $S$  be a finite set of integers with  $|S| > 1$  and let  $d$  be the greatest common divisor of all  $a - a'$  with  $a, a' \in S$ . For any  $d$ -progression  $T$ , the relation  $R_T$  is pp-definable in  $(\mathbb{Z}; \text{succ}, R_S)$ .*

PROOF: The set of maximal  $d$ -progressions contained in  $S$  can be totally ordered by setting  $T_1 \leq T_2$  if  $\min(T_1) \leq \min(T_2)$ . If  $T_1 < T_2$  then we define the distance from  $T_1$  to  $T_2$  to be  $\min(T_2) - \max(T_1)$ .

A  $d$ -progression is *non-trivial* if it contains at least two elements. For any  $m \geq 1$ , let  $(R_S)^m$  be the relation  $\overbrace{R_S \circ R_S \circ \dots \circ R_S}^m$  which we can write as  $R_{S^m}$  where  $S^m$  contains all integers that we can express as  $a_1 + \dots + a_m$  with  $a_1, \dots, a_m \in S$ . By the definition of  $d$  it follows that if  $m$  is large enough there exists some integer  $a$ , such that  $\{a, a + d\} \subseteq S$ , or, in other words, that  $S^m$  contains a non-trivial  $d$ -progression. For ease of notation we shall assume that  $S$  already contains a non-trivial  $d$ -progression (otherwise replace  $S$  by  $S^m$ ).

For any  $m \geq 1$ , let  $n_m$  be the maximum distance between two consecutive non-trivial maximal  $d$ -progressions contained in  $S^m$ . Also, let  $l_m^-$  (resp.  $l_m^+$ ) be minimum (resp. maximum) with the property that  $\{\min(S^m) + l_m^-, \min(S^m) + l_m^- + d\} \subseteq S^m$  (resp.  $\{\max(S^m) - l_m^+, \max(S^m) - l_m^+ - d\} \subseteq S^m$ ). Finally define  $l_m$  to be  $\max(l_m^-, l_m^+)$ . For ease of notation we shall write  $S^1 = S$ ,  $l_1^- = l^-$  and so on.

*Claim 1.*  $l_2 \leq l$ . Proof: Follows from the fact that  $\{2\min(S) + l^-, 2\min(S) + l^- + d, 2\max(S) - l^+ - d, 2\max(S) - l^+\} \subseteq S^2$ .

*Claim 2.* If  $l = 0$  then  $n_2 < n$ .

Proof: Let  $X < Y$  be consecutive non-trivial maximal  $d$ -progressions contained in  $S^2$ . We claim that there exist non-trivial maximal  $d$ -progressions  $A \leq B$  in  $S$  such that  $\max(A) + \max(B) \leq \max(X)$ . Indeed, set  $A = B$  to be the maximal  $d$ -progression containing  $\{\min(S), \min(S) + d\}$ . Consequently, we can choose  $A \leq B$  satisfying the conditions of the claim with  $\max(A) + \max(B)$  maximal.

Since  $X < Y$  it follows that  $\max(A) < \max(S)$  which implies that there exists a maximal  $d$ -progression  $C$  in  $S$  with  $B < C$  (in particular consider the one containing  $\{\max(S) - d, \max(S)\}$ ). Pick any such  $C$  with  $\min(C)$  minimal.

Since  $S$  contains  $d$ -progressions  $A$  and  $B$  it follows that  $S^2$  contains the (not necessarily maximal) non-trivial  $d$ -progression  $[\min(A) + \min(B), \max(A) + \max(B)]_d$ . Let  $X'$  be a maximal progression in  $S^2$  containing it. Similarly let  $Y'$  be a maximal  $d$ -progression in  $S^2$  containing  $[\min(B) + \min(C), \max(B) + \max(C)]_d$ . By the choice of  $A$ ,  $B$ , and  $C$  it follows that  $X' \leq X$  and  $X < Y'$ . As  $Y$  is consecutive to  $X$  it follows that  $Y \leq Y'$ . We finish by proving that the distance from  $X'$  to  $Y'$ ,  $\min(B) + \min(C) - \max(A) + \max(B)$ , is strictly smaller than  $n$ . Indeed, by the minimality of  $C$ ,  $\min(C) - \max(A) \leq n$  and since  $B$  is non-trivial  $\max(B) - \min(B) > 0$ . This finishes the proof of Claim 2.

Let  $T$  be any arbitrary  $d$ -progression and let  $r$  be its size. From claim 1 and 2 it follows that the value of  $l$  does not increase if we replace  $S$  by  $S^2$ . Since  $\max(S) - \min(S)$  certainly increases it follows that we can assume (by replacing  $S$  by  $S^m$  for sufficiently large  $m$ ) that  $\max(S) - \min(S) \geq 3l + (r-1)d$ . By applying iteratively claim 2 to  $S' = S \cap [\min(S) + l^-, \max(S) - l^+]_d$  we conclude that  $S^{2^n}$  contains the  $d$ -progression  $S'^{2^n} = [2^n(\min(S) + l^-), 2^n(\max(S) - l^+)]_d$ . The result follows by applying Lemma 35 to  $S^{2^n}$ . ■

**Proposition 37** *Let  $\Gamma$  be a structure with only binary relations of finite degree with a first-order definition in  $(\mathbb{Z}; \text{succ})$ . Then either  $\Gamma$  is preserved by a modular median, or  $\text{CSP}(\mathbb{Z}; \text{succ})$  is NP-hard.*

PROOF: Assume first that  $\Gamma$  contains some relation  $R_S$  for  $S = \{a_1, \dots, a_k\}$ ,  $a_1 < \dots < a_k$ , that is not a  $d$ -progression for any  $d$ . Then there exists some  $i$  such that  $a_i - a_{i-1} \neq a_{i+1} - a_i$ . Let  $d$  be the gcd. of all  $a_i - a_j$  with  $i, j \in \{1, \dots, k\}$ . By Lemma 36, relation  $R_{[a_{i-1}, a_i]_d}$  is pp-definable. Then we obtain  $R_{\{a_{i-1}, a_i\}}$  with  $R_{[a_{i-1}, a_i]_d} \cap R_S$ . Similarly one obtains  $R_{\{a_i, a_{i+1}\}}$ . The result follows from Lemma 34. Hence we are left with the case in which  $\Gamma$  contains  $d$ -progression  $R_S$  and  $d'$ -progression  $R_T$  with  $d \neq d'$ . Fix arbitrary integers  $a, b$ . In a similar way to the previous case, one can pp-define  $R_{\{a, a+d\}}$  and  $R_{\{b, b+d\}}$ . We apply again Lemma 34 to conclude the proof. ■

PROOF: (of Theorem 31) Assume  $\Gamma$  is not preserved by a modular median. We can assume that there exists some  $d > 0$  such that every binary relation pp-definable in  $(\Gamma, \text{succ})$  is a  $d$ -progression, otherwise we are done by Proposition 37. Let  $S$  be any relation in  $\Gamma$ . If  $S$  is 2-decomposable then  $S$  is invariant under  $m_d$ . Consequently, there is a relation  $S$  in  $\Gamma$  that is not 2-decomposable. This implies that, by projecting out coordinates from  $S$ , we can obtain a relation  $R$  of arity  $r \geq 3$  which is not  $(r-1)$ -decomposable. This implies, in particular, that there exists a tuple  $(a_1, \dots, a_r) \notin R$  such that for all  $1 \leq i \leq r$ ,  $(a_1, \dots, a_{i-1}, p_i, a_{i+1}, \dots, a_r) \in R$  for some integer  $p_i$ . By replacing  $R$  by the pp-defined relation

$$\exists y_1, \dots, y_r. \bigwedge_{1 \leq i \leq r} (y_i = x_i + a_i) \wedge R(x_1, \dots, x_r)$$

we can further assume that  $a_i = 0$  for all  $1 \leq i \leq r$ . Furthermore, we can also assume that for all  $1 \leq i \leq r$ ,  $p_i \in \{-d, d\}$ . Indeed let  $1 \leq i \leq r$  with  $p_i > 0$  and assume  $p_i$  is minimal. Note that  $p_i$  is a multiple of  $d$  since otherwise for any  $j \neq i$ , the projection of  $R$  to  $\{i, j\}$  would not be a  $d$ -progression. Define  $S_i$  to be the  $d$ -progression  $[0, p_i - d]_d$ . Then the relation pp-defined by the formula

$$\exists y_i. R_{S_i}(x_i, y_i) \wedge R(x_1, \dots, x_{i-1}, y_i, x_{i+1}, \dots, x_r) .$$

satisfies the condition at coordinate  $i$ . If  $p_i < 0$  one only needs to define  $S_i$  to be the  $[p_i + d, 0]_d$  and proceed in the same way.

We claim that we can pp-define a relation  $U$  of arity  $\geq 3$  such that  $(0, \dots, 0) \notin U$  and  $\{(u, 0, 0, \dots, 0), (0, u, 0, \dots, 0), (0, 0, u, \dots, 0)\} \subseteq U$  for  $u = d$  or  $u = -d$ .

Let  $P$  be the set of all  $1 \leq i \leq r$  such that  $p_i = d$  and let  $N$  be  $\{1, \dots, r\} \setminus P$ . If  $\max(|P|, |N|) \geq 3$  then we are done as  $U$  can be obtained by permuting the coordinates of  $R$ .

Otherwise, as  $r \geq 3$  we can pick  $i \in N$  and  $j \in P$ . The desired relation  $U$  can be obtained by permuting the coordinates of the  $(2r-1)$ -ary relation defined by

$$\exists x, y. (y = x + d) \wedge R(x_1, \dots, x_{i-1}, x, x_i, \dots, x_r) \wedge R(y_1, \dots, y_{j-1}, y, y_j, \dots, y_r) \wedge R_{[0, d]_d}(z, y).$$

Consider the relation  $V$  over domain  $\{0, d\}$  given by

$$\{(x, y, z) \in \{0, d\}^3 \mid (x, y, z, 0, \dots, 0) \in U\}.$$

By its construction we have that  $(0, 0, 0)$  (and hence  $(d, d, d)$ ) is not in  $V$ . Assume first that  $\{(d, 0, 0), (0, d, 0), (0, 0, d)\} \in U$  (the case  $\{(-d, 0, 0), (0, -d, 0), (0, 0, -d)\} \in U$  is analogous). It follows that  $V$  does not belong to any of the six Schaefer classes, and, hence, that the boolean  $\text{CSP}(\{0, d\}; V)$  is NP-complete. We shall show that  $\text{CSP}(\{0, d\}; V)$  reduces to  $\text{CSP}(\mathbb{Z}; \text{succ}, U)$ .

Let  $\Phi$  be an input instance of  $\text{CSP}(V)$  with variables  $X$  and let  $\phi$  be the quantifier-free part of  $\Phi$ . We construct an instance  $\Phi'$  of  $\text{CSP}(\mathbb{Z}; \text{succ}, V)$  in the following way: The set of variables of  $\Phi$  is  $X \cup \{y\}$  where  $y$  is a new variable not occurring in  $X$ . For every atomic formula  $V(x_1, x_2, x_3)$  in  $\phi$  we include in the quantifier-free part,  $\phi'$ , of  $\Phi'$  the conjunction

$$\bigwedge_{1 \leq i \leq r} R_{\{0, d\}}(y, x_i) \wedge U(x_1, x_2, x_3, y, \dots, y)$$

Clearly  $\phi'$  has a satisfying assignment if it has one setting  $y$  to 0. Also an assignment of the variables of  $\phi'$  setting  $y$  to 0 satisfies  $\phi'$  if and only if its restriction to  $X$  satisfies  $\phi$ . ■

**Proof of Theorem 1.** Suppose that  $\Gamma$  does not have a finite core. Let  $\Delta$  be the substructure of  $\Gamma$  as described in Theorem 19. Clearly,  $\text{CSP}(\Gamma)$  and  $\text{CSP}(\Delta)$  are the same problem. Unless  $\text{CSP}(\Gamma)$  is NP-hard, the relation  $\text{succ}$  is pp-definable in  $\Delta$ . By the fundamental theorem of pp definability, the CSP of the expansion of  $\Delta$  by the successor relation has the same complexity as  $\text{CSP}(\Delta)$ . Now the claim follows from Theorem 31. ■

## 7 Concluding Remarks

Structures with a first-order definition in  $(\mathbb{Z}; \text{succ})$  have a *transitive* automorphism group, i.e., for every  $x, y \in \mathbb{Z}$  there is an automorphism of  $\Gamma$  that maps  $x$  to  $y$ . We call such structures  $\Gamma$  *transitive* as well. It is well-known and easy to prove (see e.g. [15]) that a finite core of a transitive structure is again transitive. It follows from the main result obtained in our work that a complete classification of the computational complexity of finite degree distance problems would follow from a classification of the complexity of transitive finite CSPs.

In general, the complexity of the CSP for finite transitive templates has not yet been classified. The following is known.

**Theorem 38 (of [8])** *Let  $\Gamma$  be a finite core. If there is a primitive positive interpretation of the structure  $\Delta := (\{0, 1\}; \{(0, 0, 1), (0, 1, 0), (1, 0, 0)\})$  in  $\Gamma$ , then  $\text{CSP}(\Gamma)$  is NP-complete.*

The following conjecture is widely believed in the area.

**Conjecture 39 (of [8])** *Let  $\Gamma$  be a finite core. If there is no primitive positive interpretation of the structure  $\Delta := (\{0, 1\}; \{(0, 0, 1), (0, 1, 0), (1, 0, 0)\})$  in  $\Gamma$ , then  $\text{CSP}(\Gamma)$  is in P.*

We believe that this conjecture might be easier to show for *transitive* finite cores only. Note that by transitivity, the polymorphism algebra of  $\Gamma$  has no proper subalgebras. Since  $\Gamma$  is a core, all polymorphisms are surjective. It follows from known results [8] that, unless  $\text{CSP}(\Gamma)$  admits a primitive positive interpretation of  $\Delta$ , all minimal factors of the polymorphism algebra contain an affine operation.

## References

- [1] Manuel Bodirsky. Cores of countably categorical structures. *Logical Methods in Computer Science*, 3(1):1–16, 2007.
- [2] Manuel Bodirsky, Hubie Chen, and Michael Pinsker. The reducts of equality up to primitive positive interdefinability. *Journal of Symbolic Logic*, 75(4):1249–1292, 2010.
- [3] Manuel Bodirsky and Martin Grohe. Non-dichotomies in constraint satisfaction complexity. In *Proceedings of ICALP’08*, pages 184–196, 2008.
- [4] Manuel Bodirsky, Martin Hils, and Barnaby Martin. On the scope of the universal-algebraic approach to constraint satisfaction. In *Proceedings of LICS’10*, 2010.
- [5] Manuel Bodirsky and Jan Kára. The complexity of temporal constraint satisfaction problems. *Journal of the ACM*, 57(2), 2009. An extended abstract appeared in the proceedings of STOC’08.
- [6] Manuel Bodirsky and Jaroslav Nešetřil. Constraint satisfaction with countable homogeneous templates. *Journal of Logic and Computation*, 16(3):359–373, 2006.
- [7] Manuel Bodirsky and Michael Pinsker. Schaefer’s theorem for graphs. In *Proceedings of STOC’11*, 2011. Preprint of the long version available from <http://www.dmg.tuwien.ac.at/pinsker/>.
- [8] Andrei Bulatov, Andrei Krokhin, and Peter G. Jeavons. Classifying the complexity of constraints using finite algebras. *SIAM Journal on Computing*, 34:720–742, 2005.
- [9] Peter J. Cameron. *Oligomorphic Permutation Groups*. Cambridge Univ. Press, Cambridge, 1990.
- [10] Nadia Creignou, Phokion G. Kolaitis, and Heribert Vollmer, editors. *Complexity of Constraints - An Overview of Current Research Themes [Result of a Dagstuhl Seminar]*, volume 5250 of *Lecture Notes in Computer Science*. Springer, 2008.
- [11] Reinhard Diestel. *Graph Theory, 3rd edition*. Springer–Verlag, New York, 2005.
- [12] Tomás Feder and Moshe Vardi. The computational structure of monotone monadic SNP and constraint satisfaction: A study through Datalog and group theory. *SIAM Journal on Computing*, 28:57–104, 1999.
- [13] Shawn Hedman. *A First Course in Logic: An Introduction to Model Theory, Proof Theory, Computability, and Complexity (Oxford Texts in Logic)*. Oxford University Press, Inc., New York, NY, USA, 2004.
- [14] Pavol Hell and Jaroslav Nešetřil. On the complexity of H-coloring. *Journal of Combinatorial Theory, Series B*, 48:92–110, 1990.
- [15] Pavol Hell and Jaroslav Nešetřil. *Graphs and Homomorphisms*. Oxford University Press, Oxford, 2004.
- [16] Wilfrid Hodges. *A shorter model theory*. Cambridge University Press, Cambridge, 1997.

- [17] Peter Jeavons, David Cohen, and Martin Cooper. Constraints, consistency and closure. *Artificial Intelligence*, 101(1-2):251–265, 1998.
- [18] Peter Jeavons, David Cohen, and Marc Gyssens. Closure properties of constraints. *Journal of the ACM*, 44(4):527–548, 1997.
- [19] David Marker. *Model Theory: An Introduction*. Springer, New York, 2002.
- [20] Omer Reingold. Undirected connectivity in log-space. *Journal of the ACM*, 55(4), 2008.